Pozostały czas 0:08:36

Pytanie 1

Nie udzielono odpowiedzi

Punkty maks.: 1,00

Oflaguj pytanie

What is the meaning of perfect forward secrecy? Choose the best answer.

- a. Allows cryptographic separation of simultaneous sessions by using unique session keys.
- b. Means that the loss of the master secret (the master key) compromises past sessions.
- c. Means that the loss of a session key compromises future sessions.
- d. Means that the loss of the master secret (the master key) compromises future sessions.

Odznacz mój wybór

A

Pytanie 2

Nie udzielono odpowiedzi

Punkty maks.: 1,00

Oflaguj pytanie

What is the main security enhancement of WPA3? Choose the best answer.

- a. Offline attacks are impossible.
- b. The RC4 stream cipher is used.
- c. X.590 certificates are mandatory.

Odznacz mój wybór

A (aczkolwiek jest to błędne, bo nie są niemożliwe tylko utrudnione)

Which statement about X.509 certificates is true? Choose the best answer.

- a. They allow the owner of the public key to digitally sign documents in a way, that these signatures can be verified by anyone with the corresponding private key.
- b. They allow anyone to send a message encrypted with the private key, extracted from the certificate, such that only the owner of the public key can decrypt.
- c. They are used for digital signatures of digital documents.

Odznacz mój wybór

C

Which of the following statements about DIAMETER is **not true**? Choose the best answer.

- a. Next generation AAA protocol
- b. Derived from RADIUS
- c. Provides capability negotiation and error handling
- d. Uses UDP

Odznacz mój wybór

D (w przeciwieństwie do RADIUS, używa TCP lub SCTP)

Which statement describes EAP methods? Choose the best answer.

- a. They are executed in sequence or in parallel.
- b. They are specific authentication protocols, based on known algorithms or schemas.
- c. They are packet encapsulation mechanisms for the support of tunneling.

Odznacz mój wybór

B

What is the role of the Network Access Server in RADIUS? Choose the best answer.

- a. Passes user information to RADIUS server
- b. Proxy client to other RADIUS servers
- c. Authenticates the user
- d. Provides API for using secure sockets

Odznacz mój wybór

A

Which of the following describes Ephemeral Diffie-Hellman? Choose the best answer.

- a. It ensures that each time the same parties do a DH key exchange, they end up with the same shared secret.
- b. It addresses the problem of always using the same Diffie-Hellman private keys when establishing shared secret.
- c. It ensures that the same key is used multiple times.
- d. It disables perfect forward secrecy.

Odznacz mój wybór

B

Which statement about the Internet Key Exchange is true? Choose the best answer.

- a. It allows for the negotiation of EAPoL security associations (SAs).
- b. It is known for its high interoperability, ease of use, and simple design.
- c. It has been introduced as a part of the IEEE 802.11 standard.
- d. It is used to negotiate the parameters of and manage an IPSec tunnel.

Odznacz mój wybór

D

Which of the following statements are true about PEAP and EAP-TTLS? Choose the best answer.

- a. PEAP is incompatible with RADIUS.
- b. PEAP is distinct in that it secures the second phase with a TLS session.
- c. They both consist of two phases.

Odznacz mój wybór

C

Complete the sentence. Choose the best answer.

Integrity means...

- a. maintaining data consistency.
- b. that sender of a message can not deny that they sent a message.
- c. assurance of identity of a person or message originator.
- d. protection from disclosure to unauthorized persons.

a

Which of the following statements are not true regarding asymmetric cryptography? Choose the best answer.

- a. Once a key is used to encrypt a message, the same key cannot be used to decrypt the message.
- b. The overall speed of cryptographic operations is slower than in symmetric cryptography.
- c. RSA and AES are examples of algorithms used in asymmetric cryptography.
- d. Asymmetric cryptography uses two mathematically related digital keys.

c

Complete the sentence. Choose the best answer.

Authenticity means...

- a. access policy determines and grants the rights to perform some action based on identity.
- b. that sender of a message can not deny that they sent a message.
- c. protection from disclosure to unauthorized persons.
- d. assurance of identity of a person or message originator.

d

Select the stream cipher from the list below:

- a. 3DES
- b. Blowfish
- c. RC4
- d. AES

c

AES, a variant of the Rijndael block cipher standardized by NIST in 2001, stands for:

- a. Advanced Electronic Signature
- b. Advanced Encryption Standard
- c. Automated Enforcement System
- d. Acoustic Echo Suppression

b

Complete the sentence. Choose the best answer.

Non-repudiation means...

- a. that sender of a message can not deny that they sent a message.
- b. protection from disclosure to unauthorized persons.
- c. maintaining data consistency.
- d. assurance of identity of a person or message originator.

A

In secure communication scenarios, it is common to have Alice and Bob communicating over an insecure channel. In such a scenario, how is the attacker typically called? Choose the best answer.

- a. Cerberus
- b. Lilith
- c. Eve
- d. Boruta

C

What is the definition of a nonce? Choose the best answer.

- a. Defines the constant key length in stream ciphers.
- b. It used as a message authentication code.
- c. Provides user authentication.
- d. A random bitstring used only once.

D

Which is not a cryptographic requirement for hash algorithms? Choose the best answer.

- a. Second collision resistant
- b. Pre-image resistant
- c. Second pre-image resistant
- d. Collision resistant

A

In cryptography, RSA is an acronym for...

- a. Robust Security Architecture
- b. Rivest Shamir Adleman
- c. RetroSecurity Analysis
- d. Remote Stereophotogrammetric Analysis

C